УДК 654.924

А. В. Тельный, О. Р. Никитин, И. В. Храпов

ОБ ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ РАСПРЕДЕЛЕННОЙ СРЕДЫ ИНТЕГРИРОВАННЫХ СИСТЕМ ОХРАНЫ И БЕЗОПАСНОСТИ

Представлены критерии оценки и способы организации информационного обмена в распределенной информационной среде интегрированных систем охраны и безопасности различных производителей.

Ключевые слова: *интегрированные системы безопасности, SCADA-системы.*

Актуальность задачи обеспечения информационного обмена между интегрированными системами безопасности (ИСБ) разных производителей определяется [1, 2]:

— необходимостью оборудования или дооборудования объекта техническими средствами охраны и безопасности в результате строительных перепланировок, ремонтных работ и т.д.;

— развитием телекоммуникационных систем, технически позволяющих объединять в информационную систему безопасности (с созданием единого центра и единого автоматизированного рабочего места (АРМ) ИСБ) пространственно-распределенные объекты, на которых установлены ИСБ различных производителей.

Заметим, что использование одной организацией на распределенных объектах различных АРМ ИСБ, не поддерживающих информационного обмена между собой, экономически нецелесообразно, требует дополнительных затрат на обслуживание и обучение персонала, снижает уровень контроля безопасности объектов в целом.

Для небольших объектов использование нескольких программных комплексов оказывается избыточным, требует дополнительного штата сотрудников. В настоящее время развитие получили концепции „умный дом“, или „интеллектуальное здание“, интегрирующие на одной аппаратно-программной платформе и едином АРМ диспетчеризации объекта подсистемы

управления инженерно-технологическим оборудованием здания, учета потребляемых ресурсов, ИСБ.

Для обеспечения информационного обмена между ИСБ разные производители систем принимают различные технические решения, зависящие от:

— используемых аппаратно-программных средств линейки оборудования ИСБ;

— ранее разработанных АРМ ИСБ и обязательств по их технической поддержке;

— наличия и уровня подготовки специалистов в области информационных технологий;

— проводимой организацией маркетинговой политики.

Анализ технических решений производителей ИСБ показывает, что разработчики оборудования и программного обеспечения (ПО) в основном используют следующие подходы:

1) создают под платформу своего ПО ИСБ программные драйверы для возможности подключения оборудования других производителей (например, ПО „Интеллект“ фирмы ITV, Москва, содержит около 40 драйверов для различных систем). Такой вариант возможен как по соглашению между разработчиками программной платформы и оборудования ИСБ, так и без соглашения (вскрытие протоколов) по инициативе заказчика или монтажной организации при проведении пусконаладочных работ на объекте;

2) используют контроллеры, запрограммированные сторонним производителем по соглашению между разработчиками, например, сервисный модуль Ultima-EXT-i от ООО „Итриум СПб“, Санкт-Петербург, для интеграции с ИСБ „Орион-Про“ и ИСБ „Стрелец“ или модули IntesisBox для протоколов ModBus производства ООО „Солитон“, Киев, Украина;

3) используют программируемые промышленные контроллеры или преобразователи интерфейсов (протоколов) различных производителей, которые программируются заказчиком или монтажной организацией при проведении пусконаладочных работ на объекте;

4) разработчики ПО ИСБ выпускают платформы с открытой архитектурой для того, чтобы пользователи могли самостоятельно в АРМ ИСБ обмениваться с ИСБ других производителей (например, на основе протокола ModBus);

5) разработчики линейки ИСБ создают для своего оборудования программируемые модули и OPC-серверы, предоставляют протоколы ModBus или используют протоколы стандарта LONWORKS с промышленно выпускаемыми контроллерами (например, фирмы Echelon). Такой подход позволяет полнофункционально интегрировать различные ИСБ на основе SCADA-платформ;

6) разработчики ИСБ интегрируют свои продукты на основе менее распространенных и более закрытых информационных технологий с использованием SCADA-платформ (пример — технология COBRA).

Оценив достоинства и недостатки каждого из технических подходов к интеграции информационного обмена между ИСБ, можно сказать, что наиболее перспективным представляется их интеграция на основе SCADA-платформ с использованием контроллеров и серверов, выпускаемых производителем оборудования по следующим причинам:

1) при программировании контроллеров заказчиком или монтажной организацией, создании драйверов оборудования ИСБ необходим высокий уровень подготовки специалистов во избежание возможных ошибок. Программисты, как правило, не являются специалистами в области эксплуатации ИСБ;

2) созданные программные продукты должным образом и в необходимом объеме не тестируются, у заказчика может не быть таких возможностей;

3) при самостоятельном создании драйверов (программировании контроллеров) без соглашения с производителем и получения от разработчиков полной информации о протоколах обмена (вскрытии протоколов) возможны критические ошибки и возникновение уязвимостей в функционировании ИСБ, о которых заказчик может не знать;

4) при обновлении линейки оборудования разработчику ИСБ, возможно, придется заново программировать контроллеры, что для заказчика экономически невыгодно. В то же время обновление драйверов от разработчика осуществляется, как правило, в порядке технической поддержки;

5) при самостоятельной разработке драйверов (программировании контроллеров) возможно неумышленное создание опасности проникновения злоумышленников в распределенную информационную систему;

6) при использовании универсального ПО ИСБ с внедренными драйверами для подключения оборудования различных производителей заказчик оказывается „привязанным“ к выбранной платформе ПО, интерфейсу пользователя, сервису ПО и т.д. Техническая поддержка драйверов (обновления) сторонним производителем ПО ИСБ, как правило, не осуществляется.

SCADA-системы поддерживают разные типы контроллеров автоматики зданий, но не поддерживают контроллеры, применяемые для систем безопасности. Для подключения контроллера к SCADA-системе требуется разработка OPC-сервера. На данный момент наиболее распространен стандарт OPC DA Version 2.05a.

OPC-набор спецификаций стандартов. Каждый стандарт описывает набор функций определенного назначения. Текущие стандарты:

— OPC DA (Data Access) — основной и наиболее востребованный стандарт. Описывает набор функций обмена данными в реальном времени с ПЛК, РСУ, ЧМИ, ЧПУ и другими устройствами;

— OPC AE (Alarms & Events) — предоставляет функции уведомления о различных событиях (аварийных ситуациях, действиях оператора, информационных сообщениях и др.) по требованию;

— OPC Batch — предоставляет функции шагового и рецептурного управления технологическим процессом (в соответствии со стандартом S88.01);

— OPC DX (Data eXchange) — предоставляет функции организации обмена данными между OPC-серверами через сеть Ethernet. Основное назначение — создание шлюзов для обмена данными между устройствами и программами разных производителей;

— OPC HDA (Historical Data Access) — предоставляет доступ к сохраненным данным;

— OPC Security — определяет функции организации прав доступа клиентов к данным системы управления через OPC-сервер;

— OPC XML-DA (XML-Data Access) — предоставляет гибкий, управляемый правилами формат обмена данными через SOAP и HTTP;

— OPC UA (Unified Architecture) — последняя по времени выпуска спецификация, которая основана не на технологии Microsoft COM, что предоставляет кроссплатформенную совместимость. Еще одна разновидность OPC-сервера — шлюз к сети полевой шины, такой как Profibus или LonWorks (обычно на компьютере с ОС Windows устанавливается адаптер fieldbus-сети, а OPC-сервер взаимодействует с этой сетью через драйвер адаптера).

Наиболее востребована программа высокого уровня OPC DA. Почти все известные SCADA-продукты являются OPC-клиентами, например, SCADA АЛГОРИТМ (БОЛИД), ЭНТЕК (ЭНТЕЛС), MasterSCADA (ИнСАТ), InTouch (Wonderware), TRACE MODE (AdAstra), Vijeo Citect (Schneider Electric), КРУГ-2000 (КРУГ), CitectSCADA (Schneider Electric), Genesis32 (ICONICS), а большинство из них и OPC-серверами (в частности, CiTect, MasterSCADA, КРУГ-2000 и TRACE MODE). Поддержка OPC HDA из российских полнофункциональных SCADA-систем реализована только в SCADA TRACE MODE, MasterSCADA и КРУГ-2000.

На отечественном рынке производителей оборудования и АРМ ИСБ в настоящее время складывается следующая ситуация по использованию интеграции систем в SCADA:

1) НВП „Болид“, Королев, ИСБ „Орион-Про“. Аппаратные средства: преобразователь протокола С2000-ПП для интеграции линейки оборудования системы „Орион“ по интерфейсу Modbus RTU. Шлюз Modbus, тип интерфейса RS-485, тип протокола Modbus-RTU. Программные средства: OPC-сервер для АРМ „Орион-Про“ (Сервер состояний: позволяет получать информацию о состоянии групп разделов, разделов, приборов, шлейфов, реле, считывателей, дверей, получать значения АЦП шлейфов, ставить и снимать с охраны разделы и шлейфы, управлять реле. Соединяется с ядром АРМ „Орион-Про“ через интерфейс XML-Rpc). OPC-сервер Orion-ModBus поддерживает интерфейс OPC DA2.0 и работает с прибором „С2000-ПП“, опрашивая его по протоколу ModBus-RTU;

2) ЗАО „Аргус-Спектр“, Санкт-Петербург: ВОРС „Стрелец“ и „Стрелец-Интеграл“. Аппаратные средства: блок преобразования интерфейсов БПИ RS-И (USB; RS232); блоки сетевых интерфейсов U.10, i.LON-10, i.LON-100, i.LON-600, PCL-TA-21, PCC-10 (Ethernet; GSM/GPRS;PCI; PCMCIA) и др. являются стандартными сетевыми интерфейсами платформы LONWORKS и производятся фирмой Echelon. Информационная среда ИСБ строится на основе стека протоколов стандарта LONWORKS LON ANSI/EIA 709.1 (EN 14908, ISO/IEC 14908). В качестве основного физического интерфейса в ИСБ используется интерфейс TP/FT-10;

3) ЗАО „Риэлта“, Санкт-Петербург, ИСБ „Ладога-А“ с использованием ПО фирмы „Eselta“. В ПО ИСБ добавлен OPC-сервер, реализующий доступ к данным и событиям Eselta благодаря технологиям OPC Data access и OPC Alarm events;

4) фирма „Сигма-ИС“, Москва, ИСБ „Рубеж-08; Р-09“. Имеется OPC-сервер к оборудованию „Рубеж“ для представления объектов технических средств (ТС) БЦП в виде тегов. Сервер разработан на основе универсального OPC-сервера фирмы FastWell (UniOPC Server);

5) фирма Honeywell (ранее Ademco) ИСБ серии VISTA и Galaxy — ПО „Compass“ (много других ПО, поддерживающих данные панели). На рынке представлено много стандартных OPC-серверов для работы с контроллерами Honeywell, например, разработанные фирмой Intesis. Intesis OPC-сервер для систем противопожарной сигнализации Notifier ID3000 series (Honeywell)-ID3000;

6) ООО „Плазма-Т“, Москва, ПО „Спрут-2“ для автоматизации пожарной сигнализации и оборудования управления противопожарной автоматикой. Имеется OPC-сервер для интегрирования комплекта „Спрут-2“ в системы диспетчерского управления и сбора данных SCADA/HMI. На сайте разработчика представлена таблица ModBus для наладки программ, поддерживающих ModBus RTU;

7) группа компаний „АСБ“, Москва, ИСБ „Пахра“, „Антел“. В ПО ИСБ „Радиосеть“ и ПО „Пахра“ использована архитектура распределенной самосинхронизирующийся среды функционирования, конфигурируемой при помощи XML. Интеграции в SCADA от производителя нет;

8) ЗАО „Теко“, Казань, ИСБ „Астра-РИМ“, „Астра-812“. Интеграции в SCADA от производителя нет;

9) фирма „Кодос“, Москва, ИСБ на основе ППКОП „Кодос А-20“. Интеграции в SCADA от производителя нет;

10) НПО „Сибирский арсенал“, Новосибирск, оборудование „Гранит“, „Карат“, ИСБ „Лавина“. Интеграции в SCADA от производителя нет;

11) ООО „Альтоника“, Москва, радиоканальные системы „Риф Стринг“ ПО „Риф Страж“. Интеграции в SCADA от производителя нет;

12) группа предприятий „Ровалент“, Минск, Беларусь, ИСБ „777“ и АРМ ИСБ „777“. Интеграции в SCADA от производителя нет.

Таким образом, выбор ИСБ при оборудовании объектов системами охраны и безопасности или выбор способа организации информационного взаимодействия между системами различных производителей необходимо осуществлять с учетом возможности объединения ИСБ

на основе SCADA-технологий. Предложенные в статье критерии оценки и способы интеграции ИСБ позволяют избежать непроизводительных финансовых затрат, повысить эффективность эксплуатации ИСБ в целом и уровень контроля функционирования ИСБ.

СПИСОК ЛИТЕРАТУРЫ

1. Системы безопасности и мониторинга — Интегрированные системы безопасности [Электронный ресурс]: <http: // rovalant.com/systems/integrated-systems.html>.

2. *Тельный А. В.* Организация взаимодействия между подсистемами интегрированной системы безопасности // Тр. X Росс. Науч.-техн. конф. „Новые информационные технологии в системах связи и управления“. Калуга: Изд-во ООО „Ноосфера“, 2011. 610 с.

Сведения об авторах

Андрей Викторович Тельный — канд. техн. наук, доцент; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: andre.izi@mail.ru

Олег Рафаилович Никитин — д-р техн. наук, профессор; Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, кафедра информатики и защиты информации; E-mail: olnikitin@mail.ru

Игорь Викторович Храпов — канд. техн. наук; Тамбовский государственный технический университет; аналитический центр экономического развития; директор; E-mail: igor@tambov.ru

Рекомендована ВлГУ

Поступила в редакцию
17.04.12 г.